**IN THE CLAIMS**

Please cancel claims 1-23 without prejudice

Please add new claims 24-46 as follows:

1-23. (Cancelled)

24. (New) A method for effectively and efficiently identifying violations of privacy and security and guidelines in an information system, comprising the steps of:

a. providing vulnerability data having universal definitions applicable to different computing systems;

b. providing regulation data relating to a particular set of regulations;

c. providing priority data relating to a list of vulnerabilities prioritized in a specific order;

d. providing keywords that are common to the vulnerability, regulation and priority data;

e. searching for the keywords in the vulnerability, regulation and priority data;

f. creating relational data based upon the searching step, the relational data establishes a specific relationship between the vulnerability, regulation and priority data;

g. determining a computer configuration for a target to be tested;

h. customizing a screening process for the target using the computer configuration found in the determining step;

i. testing for vulnerability violations in the target based upon the customized screening process;

k. determining, according to the vulnerability violations, which regulation data applies to which vulnerability data and the priority of the vulnerability violations; and

l. creating a prioritized report corresponding to the vulnerability violations and the regulations that apply to the vulnerability violations.

25. (New) The method of claim 24 wherein the set of regulations are defined by Health Insurance Portability and Accountability Act.

26. (New) The method of claim 24 wherein the set of regulations are defined by Graham Leach Bailey Act.

27. (New) The method of claim 24 wherein the vulnerability violations are stored in a memory.

28. (New) The method of claim 24 wherein the testing step further comprises scanning a target to provide a system scan.

29. (New) The method of claim 28 further comprising the step of providing a test set as a function of the system scan.

30. (New) The method of claim 24 the prioritized report further includes an IP address of the target.

31. (New) The method of claim 24 wherein the vulnerabilities data is defined by Common Vulnerabilities and Exposures.

32. (New) A information system for effectively and efficiently identifying violations of privacy and security and guidelines, comprising:

a. a vulnerability database having universal definitions applicable to different computing systems;

b. a regulation database relating to a particular set of regulations;

c. a priority database relating to a list of vulnerabilities prioritized in a specific order;

d. means for providing keywords that are common to the vulnerability, regulation and priority data;

e. searching means for searching for the keywords in the vulnerability, regulation and priority data;

f. a memory for storing relational data that was created by the searching means, the relational data establishes a specific relationship between the vulnerability, regulation and priority databases;

g. first determining means for determining a computer configuration for a target to be tested;

h. customizing means for customizing a screening process for the target using the computer configuration found in the first determining means;

i. testing means for testing for vulnerability violations in the target based upon the customized screening process;

k. second determining means for determining, according to the vulnerability violations, which regulation data applies to which vulnerability data and the priority of the vulnerability violations; and

l. a prioritized report corresponding to the vulnerability violations and the regulations that apply to the vulnerability violations.

33. (New) The system of claim 32 wherein the set of regulations are defined by Health Insurance Portability and Accountability Act.

34. (New) The system of claim 32 wherein the set of regulations are defined by Graham Leach Bailey Act.

35. (New) The system of claim 32 wherein the vulnerability violations are stored in a memory.

36. (New) The system of claim 32 wherein the testing means further comprises scanning a target to provide a system scan.

37. (New) The system of claim 36 further comprising a test set as a function of the system scan.

38. (New) The system of claim 32 wherein the prioritized report further includes an IP address of the target.

39. (New) The system of claim 24 wherein the vulnerabilities data is defined by Common Vulnerabilities and Exposures.

40. (New) Computer-executable process steps, stored on a computer-readable medium and executable by a processor to perform the steps of:

a. provide vulnerability data having universal definitions applicable to different computing systems;

b. provide regulation data relating to a particular set of regulations;

c. provide priority data relating to a list of vulnerabilities prioritized in a specific order;

d. provide keywords that are common to the vulnerability, regulation and priority data;

e. search for the keywords in the vulnerability, regulation and priority data;

f. create relational data based upon the search step, the relational data establishes a specific relationship between the vulnerability, regulation and priority data;

g. determine a computer configuration for a target to be tested;

h. customize a screening process for the target using the computer configuration found in the determine step;

i. test for vulnerability violations in the target based upon the customized screening process;

k. determine, according to the vulnerability violations, which regulation data applies to which vulnerability data and the priority of the vulnerability violations; and

l. create a prioritized report corresponding to the vulnerability violations and the regulations that apply to the vulnerability violations.

41. (New) The steps of claim 40 wherein the set of regulations are defined by Health Insurance Portability and Accountability Act.

42. (New) The steps of claim 40 wherein the set of regulations are defined by Graham Leach Bailey Act.

43. (New) The steps of claim 40 wherein the test step further comprises scanning a target to provide a system scan.

44. (New) The steps of claim 43 further comprising the step of providing a test set as a function of the system scan.

45. (New) The steps of claim 40 wherein the prioritized report further includes an IP address of the target.

46. (New) The steps of claim 40 wherein the vulnerabilities data is defined by Common Vulnerabilities and Exposures.